Особенности аутсорс-разработки финансовой системы

и почему это так больно

Антон Морев, Wormsoft





Кто я?

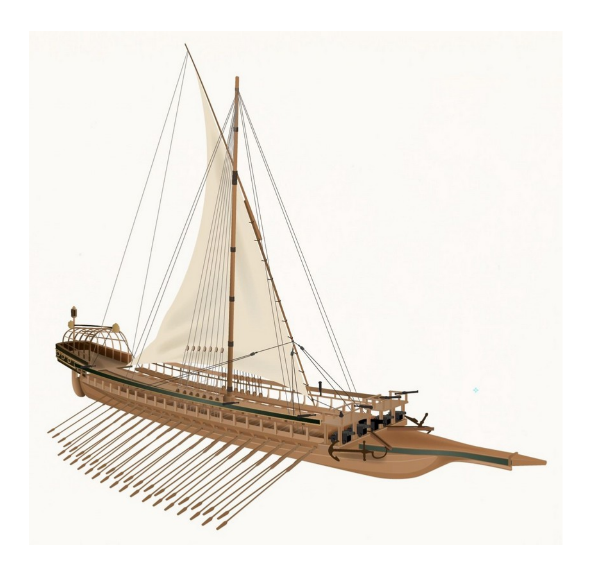


Антон Морев

- amorev.ru / Telegram канал: @amorev94
- CTO Wormsoft
- Преподаватель JS
- ПК KnowledgeConf



Кто мы?



wormsoft.ru

outsource разработка всего и вся

техподдержка и IT сопровождение

много, так или иначе, работаем с деньгами

и профессионально косячим с ними:)



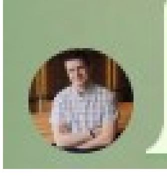
О чем доклад?

- Разбор пары реальных наших финтех проектов
- Факапы и проблемы, которые мы создали
- Способы и костыли, которыми спасались



Дисклеймер

- Дабы не было рекламы все название выдуманы
- К сожалению кейсы не выдуманы
- Заранее знаю что фейлы детские
- Иногда похоже на нытье



Деньги на этих факапах уже потеряли - сегодня буду терять репутацию)))

3 14:59



Что мы делаем?

- … страдаем



Что мы делаем?

- Криптовалютная биржа и банк
- Торговые роботы на FORTS и криптобиржах
- Системы обработки отчетностей торговых дней на фондовых биржах
- Интернет магазины, но сегодня не о них...
- Системы управления коворкингами

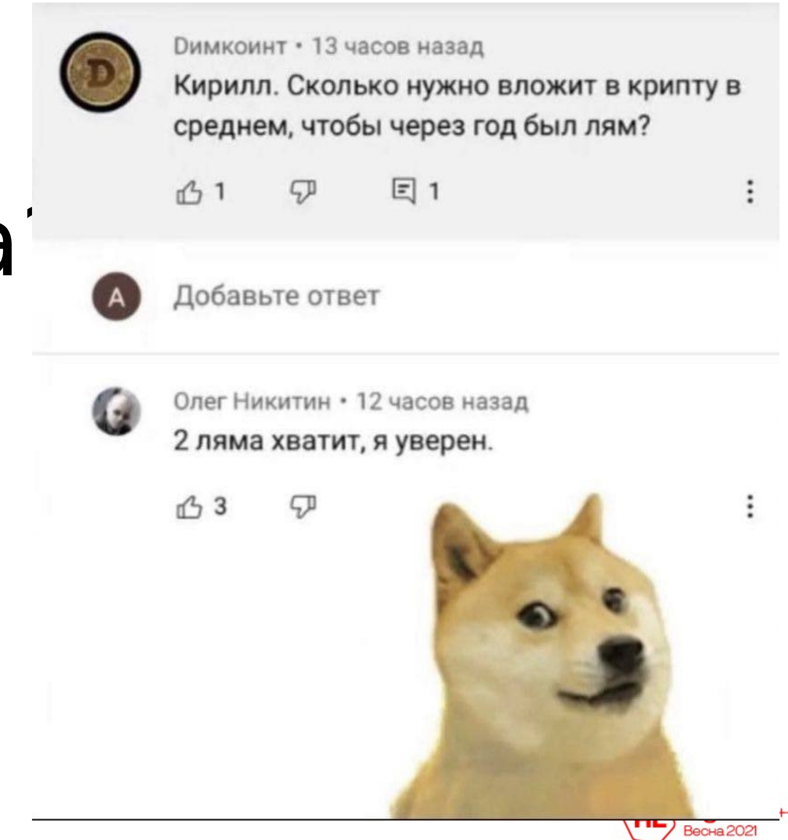


ФАКАПЫ НА КРИПТОБАНКЕ + БИРЖЕ



Вопросы без ответа

- Почему это банк?
- Почему это биржа?



Почему это банк?



Какая То Новая Монета



Почему это бан













Почему это банк?

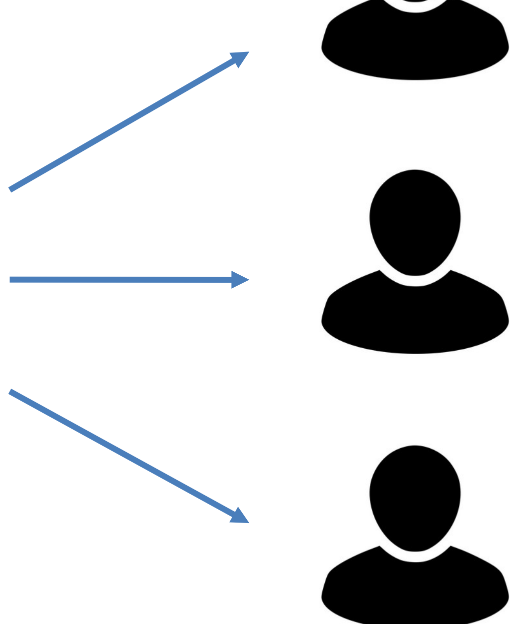








Разработанный нами сервис



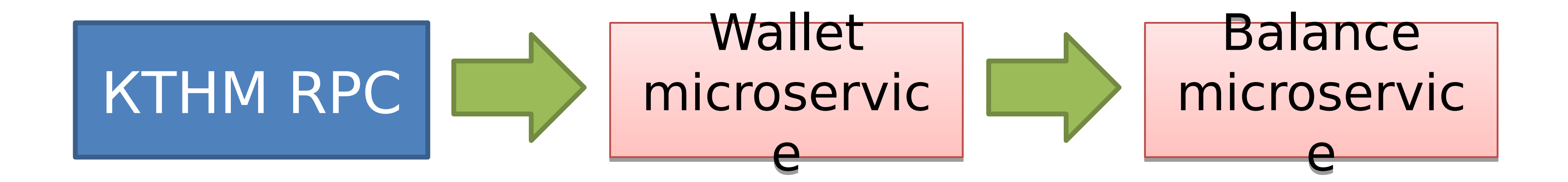


Проверка времени последнего блока

```
if (currentTime > lastBlockTime) {
    // сохраняем транзакцию
}
```



Обработка POS дохода





Обработка POS дохода

KTHM RPC

Wallet microservice

Wallet microservice

Balance microservice

19:34

22:34



Проверка времени последнего блока

```
if (currentTime > lastBlockTime) {
    // сохраняем транзакцию
}
```



Обработка POS дохода

KTHM RPC

Wallet microservice

Wallet microservice

19:34

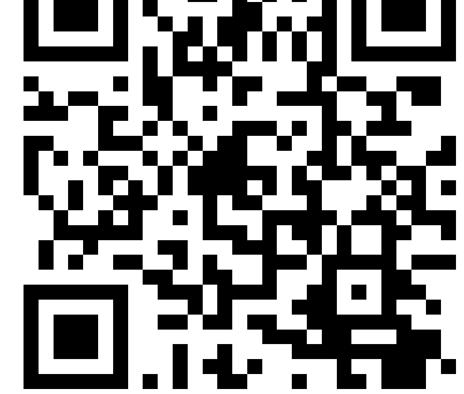
Balance microservice

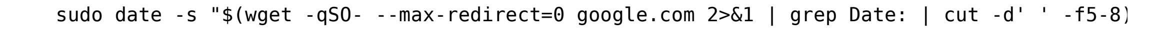
22:34



Срочное решение

- NTP не включалось, а время шло
- Вручную настроить не вариант (2FA будет сбоить)
- В ход пошел костыль..



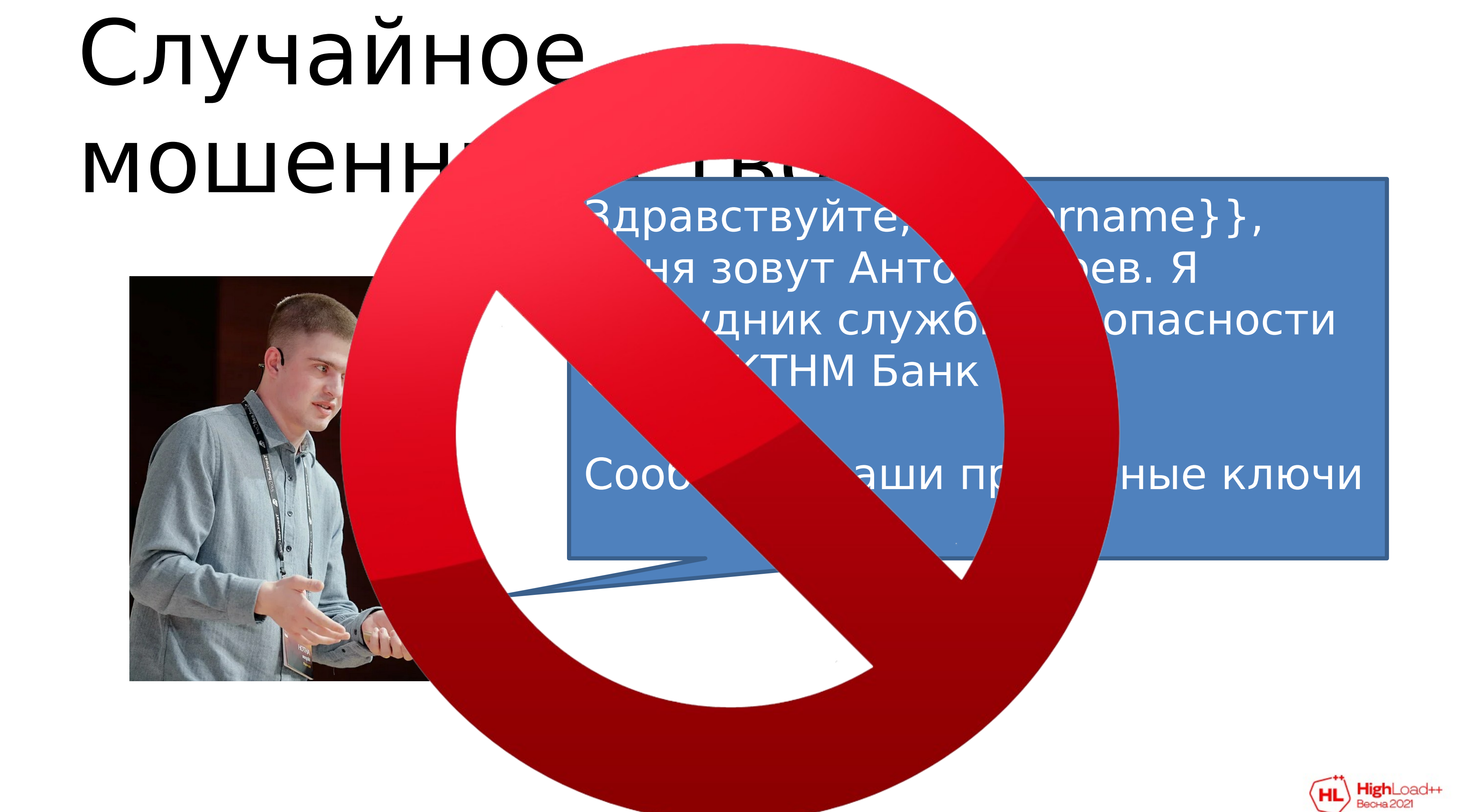




Боли аутсорса в финтехе

- Время сервера важно для транзакций





Случайное
мошенн
Здравствуйте, rname}},
ня зовут Анто ев. Я
удник служб опасности
КТНМ Банк
Сооб аши пр ные ключи
HL
HighLoad++
Весна 2021

```
create table transaction
(
    id serial,
    amount float,
    created_at int
);
```

Капитанское правило – не хранить float

0.1 + 0.2 = 0.30000000000000004

0.1 * 0.2 = 0.020000000000000004

0.1 * 0.7 = 0.06999999999999999

том нет ничего смешного, я знавал людей,
торых посадили в тюрьму за то, что они использовали тип float в БД для хранения денег
об Мартин



Случайное мошенничество

- В день около 10-15 транзакций банковской доходности **КАЖДОМУ** пользователю
- Сервис начал набирать пользователей
- Пользователи заводить деньги
- Зарабатывать POS доход, исчисляемый 0.0001 за каждую транзакци
- Пользователи недополучили



Решение

- Все числа хранить как INT
- Везде делить/умножать на 10^9
- В форме отображать уже обычный float чисто визуально



Боли аутсорса в финтехе

- Время сервера важно для транзакций
- Бежать от FLOAT, DOUBLE и тд



Вопросы без ответа

- ~~Почему это банк?~~
- Почему это биржа?

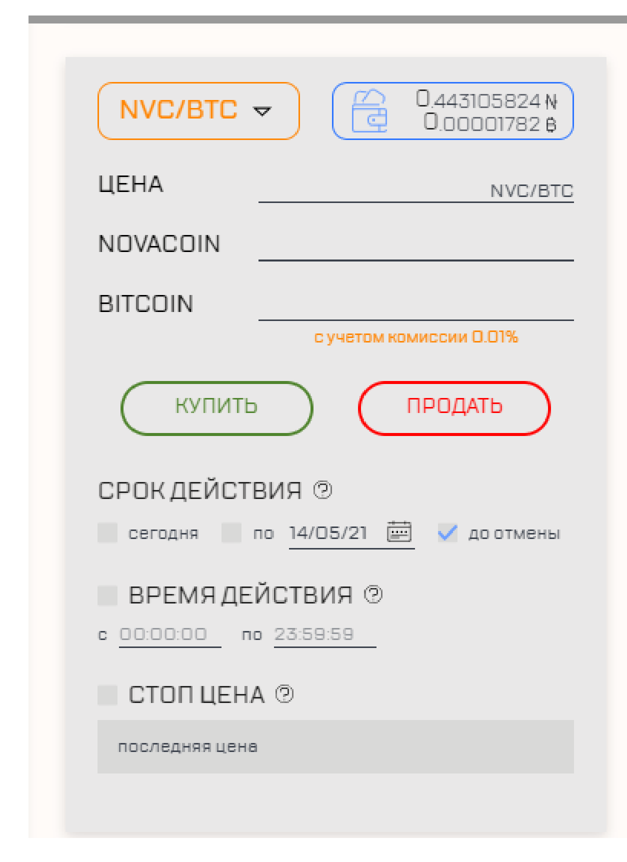


Почему это биржа?

KTHM



Почему это биржа?



СТАКАН КОТИРОВОК

ПОКУПКА	ЦЕНА	ПРОДАЖА
×	฿ 0.5	₦ 2.254597127
	฿ 0.0005	₦ 10000
	฿ 0.0004	₦ 10
	฿ 0.00007	₦ 10000
	฿ 0.00005	₦ 299.9501
₦ 131	฿ 0.000032	
₦ 4836.85909	฿ 0.00003	
₦ 3325.28820551	฿ 0.000025	
₦ 2007.69528	฿ 0.000022	
₦ 3200	฿ 0.00002	



Решение

- Все числа хранить как INT
- Везде делить/умножать на 10^9
- В форме отображать уже обычный float чисто визуально

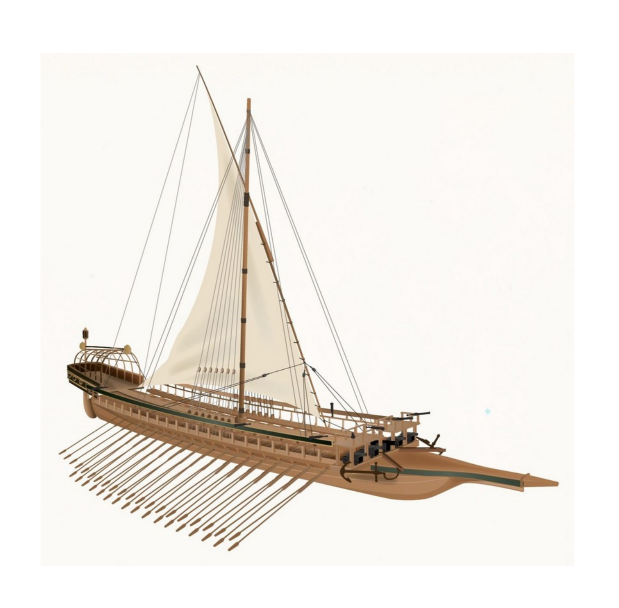


Решение **(неудачное)**

- **Все числа хранить как INT**
- Везде делить/умножать на 10^9
- В форме отображать уже обычный float чисто визуально



Валидация ввода денег









Форма заявки на биржу

NVC/BTC
0.443105824 ₦
0.00001782 ฿

ЦЕНА NVC/BTC
NOVACOIN
BITCOIN
с учетом комиссии 0.01%

КУПИТЬ ПРОДАТЬ

СРОК ДЕЙСТВИЯ
сегодня по 14/05/21 до отмены

ВРЕМЯ ДЕЙСТВИЯ
с 00:00:00 по 23:59:59

СТОП ЦЕНА
последняя цена

СТАКАН КОТИРОВОК

ПОКУПКА	ЦЕНА	ПРОДАЖА
×	[illegible]	₦ 2.254597127
	฿ 0.0005	₦ 10000
	฿ 0.0004	₦ 10
	฿ 0.00007	₦ 10000
	฿ 0.00005	₦ 299.9501
₦ 131	฿ 0.000032	
₦ 4836.85909	฿ 0.00003	
₦ 3325.28820551	฿ 0.000025	
₦ 2007.69528	฿ 0.000022	
₦ 3200	฿ 0.00002	

По какой цене
Сколько купить/продат



НЕ ХРАНИТЬ FLOAT



Форма заявки на биржу

NVC/BTC

0.443105824 Ɲ
0.00001782 ฿

ЦЕНА	0,0004	NVC/BTC
NOVACOIN	100	
BITCOIN	0,0404	

с учетом комиссии 0.01%

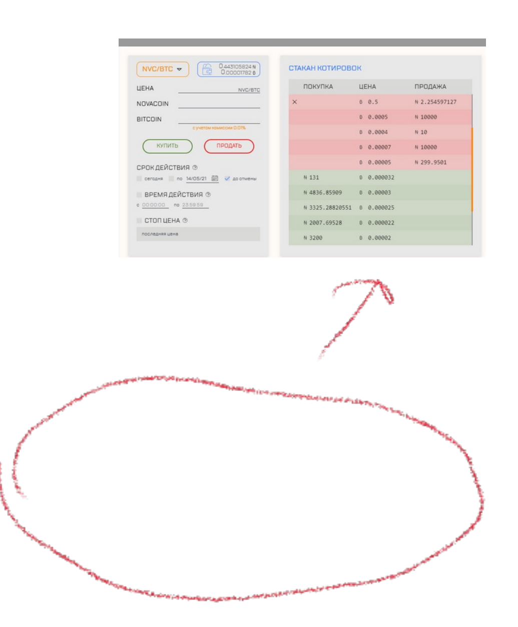
КУПИТЬ ПРОДАТЬ

СРОК ДЕЙСТВИЯ

400
10000000
40400



Order Lifecycle





Форма заявки на биржу

NVC/BTC

0.443105824 ₦
0.00001782 ฿

ЦЕНА 99999999 NVC/BTC

Не больше 1 000 000

NOVACOIN 999999999

Не больше 1 000 000

BITCOIN 10099999888900000

Не больше 1 000 000 000 000

КУПИТЬ

ПРОДАТЬ

СРОК ДЕЙСТВИЯ

сегодня по 17/05/21 до отмены



ПЕРЕПОЛНЕНИЕ

... возможно signedness error

... но это неточно



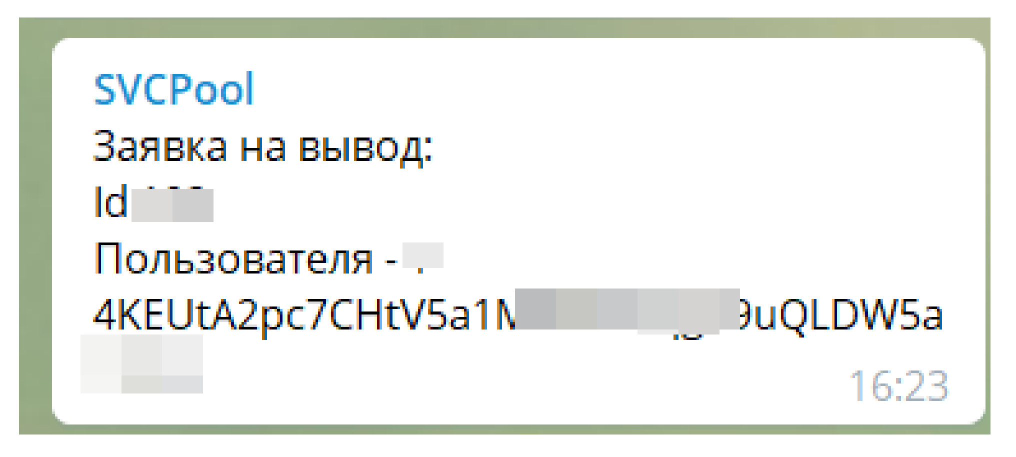
Переполнение

- Вводим огромные числа
- Amount выходит за пределы int
- И начинается непойми-что
- В итоге, путем нехитрых манипуляций, удается добиться отрицательного amount
- Пользователи кидают заявку…..

- … их баланс пополняется



Как мы поняли, что чего то не так?







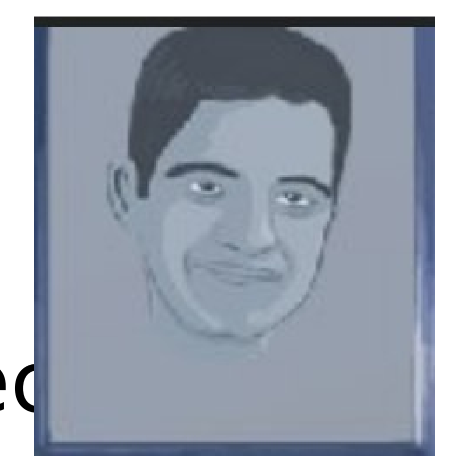
Решение

- Компенсация клиенту
- Перенос релиза
- Переход везде на big decimal



Решение

- Компенсация клиенту
- Перенос релиза
- Переход везде на big dec



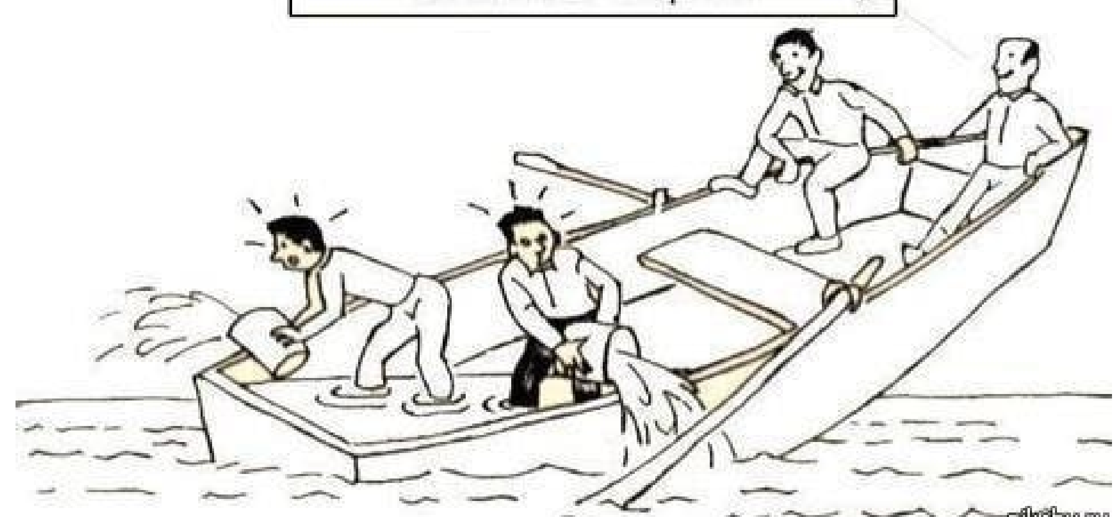
Надо было нанять еще QA



Боли аутсорса в финтехе

- Время сервера важно для транзакций
- Бежать от FLOAT, DOUBLE и тд
- Переполнение это дорого!




Здорово, что проблема не на нашей стороне
pikabu.ru


HL
HighLoad++
Весна 2021

ПРОБЛЕМЫ РАСПИЛА



Трансформация стека

PHP Yii2
Монолитный
монолит



PHP Balance Service
NodeJS BFF
NodeJS Auth
GoLang Orderbook
GoLang Wallet service



Подтверждения транзакций

- Транзакция попадает в сеть с 0 подтверждений
- Ноды сохраняют ее себе
- Проходит 6 подтверждений
- Деньги можно тратить

- Пока не будет 6 подтверждений деньги на балансе не обновятся





Пробл

Это же wormsoft

расслабься

memesmix.net

До распил а

- сервис р недолетели
- Транзакц исались
- POS зара
- Выключа

Деньги ушли

Деньги пришли

Релиз и новые адреса...

Набралось подтверждений

Можно тратить

t, время



ХРАНЕНИЕ СО ЗНАКАМИ

... не все что минус будет в минус и не все что плюс должно быть плюсом



Проект расчета результатов

Брокер

XML

Наша система

REST

Биржи (Фиатные)

Интерфейс клиентов



Предположения (не аксиомы)

- Отчеты XML – единый источник правды
- Ошибок в отчете быть не может
- Если в отчете число со знаком минус, значит вычитаем
- В отчетах учтены все транзакции
- Отчеты высылаются сегодня за вчерашний день
- Порядок имеет значение



Предположения (не аксиомы)

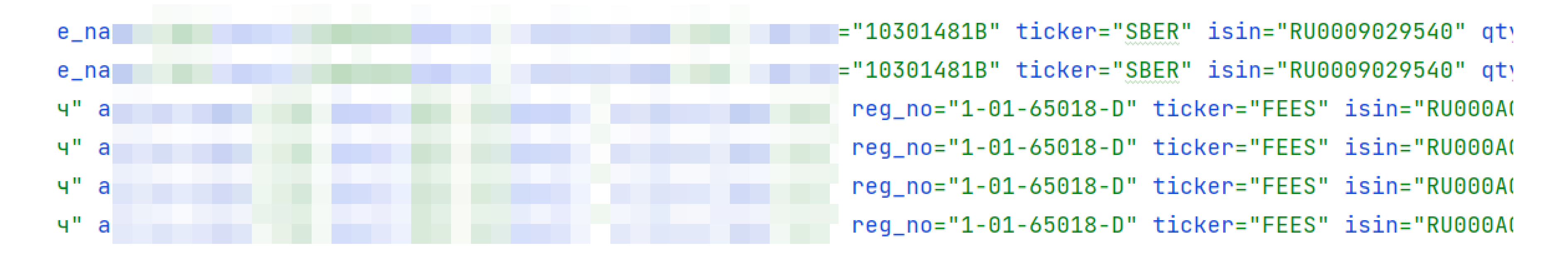
- ~~Отчеты XML – единый источник правды~~
- ~~Ошибок в отчете быть не может~~
- ~~Если в отчете число со знаком минус, значит вычитаем~~
- ~~В отчетах учтены все транзакции~~
- ~~Отчеты высылаются сегодня за вчерашний день~~
- ~~Порядок имеет значение~~



de= ai
is_signature="0"/>

" nonexch_receipt="0" loan_receipt="0" expense_amount="-2998506.24" exch_expense="-2998474.96" comm_brok="

egin_qty="17590000" end_qty="17680000" debt="-17680000" plan_end_qty="0"/>



ч" ac reg_no="1-01-65018-D" ticker="FEES" isin="RU000A



```
mount="150066631.55" exch_expense="150058717.42"     non
" comm_brok="0" comm_exch="0" nonexch_expense="0"    deb
```



Разные знаки

- Пишется система, рассчитывающая видеть минус у расходов и плюс у доходов
- Запускается система, работает, показывает клиентам их результаты
- Добавляется новый брокер, который пишет просто значение по модулю
- У клиентов отображается искаженная информация

- … беда



Боли аутсорса в финтехе

- Время сервера важно для транзакций
- Бежать от FLOAT, DOUBLE и тд
- Переполнение это дорого!
- Следить за знаками: пишем все положительное и фиксируем type



«УДОБНЫЕ» ИНТЕГРАЦИИ



Типы операций в XML

```
return [
    'Перевод между Основным и Торговым счетами ДС',
    'Перевод ДС (зачисление)',
    'Cash Transfer',
    'Перевод ДС (списание)',
    'Перевод ДС',
    'Перевод',
    'Transfer',
    'Дивиденды',
    'Dividends',
];
```




Способы доставки XML

- API эндпоинт для сбора данных
- Выкладывание на SFTP с закрытым доступом
- Отправка на email человеком в свободной форме
- Ручное выкачивание из ЛК



Боли аутсорса в финтехе

- Время сервера важно для транзакций
- Бежать от FLOAT, DOUBLE и тд
- Переполнение это дорого!
- Следить за знаками: пишем все положительное и фиксируем type
- Обычно об удобстве интеграции не думают



Благодарю за вниман



Антон Морев

amorev.ru/contact

youtube.com/amorev

@amorev94 – TG channel

